SkyeModule^{TM} M9 参考指南

- 版本 070608

公司信息
杭州紫铖科技有限公司
Ziytek,co.,ltd
杭州市文三路 90 号东部软件园 1 号楼 1221 室
1221Room,1st Floor 90# wensan Rd.
ESP, Hangzhou CHN

紫铖科技技术支持和联系信息
Ziytek Technical Support and Contact Information:
E-mail: wang.xz@ziytek.cn
Website: Http://www.ziytek.com

第一章

SkyeModule M9 概况

概述

M9 是世界上符合 ETSI302 208 协议最小的多协议超高频(862 - 955 Mhz)RFID 读写器模块，可以支持市面上绝大多数的超高频(UHF)电子标签。M9 可以对基于 EPC Class1 Gen1、ISO 18000-6B 和 ISO 18000-6C(EPC C1G2/Gen2)空中接口和协议标准的标签进行可读写操作，输出功率可以通过软件在 15mW 到 500mW 的范围内自定义调整。M9 已经通过了包括北美、欧洲和韩国等主要市场地区的检测和认证。M9 符合 RoHS

特征

基于SkyeTek独特的Common Blade读写器架构，它针对物流、消费品、手持机和标签打印机等行业应用，M9具有以下特性：

- 模块化的硬件 - 所有common blade系列读写器共享数字电路部分，这意味着任何支持其中一种Common Blade架构模块的外设也能支持该架构的其它模块。

- 通用固件 - 通用固件可以确保新的读写器特性和标签协议可以适用于所有Common Blade系列的全线产品。

- 通用机械规格 - Common Blade系列读写器模块采用相同的规格尺寸，使客户在无需改动现有的产品的前提下，可以在高频应用，具有安全要求的高频及超高频应用中自由选择和变换。

- 通电电气接口 - Common Blade系列读写器采用相同的CF卡数据接口，所有的供电和数据通信都是相同的。

- 通用主机接口 - Common Blade系列模块采用相同的微控制器通讯方式：串行TTL、SPI、和I2C，也支持通过USB方式和不具有串口的PC机进行连接。

- 通用通信协议和C语言的API - 所有Common Blade系列产品都是根据SkyeTek v3版本协议驱动通信，并提供基于该协议的C语言API及操作读写器和阅读标签的各种方法。

M9 已经过优化支持 40/80 kbps 的数据传输率，通过外接一个标准 50 欧姆的天线可以增大读写距离。

M9 提供多种主机接口选择：TTL(UART),SPI,USB和I^2C，这些方式可以通过软件选择以满足不同的松紧耦合集成要求。M9 为I/O到外设提供了 7 个的可编程GPIO引脚，连续数据传输率可以在 9.6 到 115.2kbps的范围内调整。此外，日后如需要增加新标签协议，安全特性或是客户自定义功能等，均可以通过固件升级来实现。

SkyeWare™ 软件

所有 M9 开发包里都配有 SkyeWare 软件可以在微软系统下来协助你的 RFID 开发进程。

- SkyeStart –通过该向导你可以来设置，配置和检测新阅读器。可以在 18 步内来完成配置，连接硬件，装载固件，运行诊断检测以及优化读写器配置。它配有附加 SkyeTek 软件和文档的有效链接。
- SkyeDemo – 他示范了 M9 的基本文本读写功能。你可以测试阅读范围（用 Loop Select），速度（用 Timed Select），详细目录模式和防碰撞性能（用 Inventory Select）。SkyeDemo 为 M9 基本性能的高水平示范提供了一条捷径。
- SkyeWare – 让您更简便的深度测试 M9 的性能。您可以浏览和改变阅读器的配置参数，或者执行基本的标签操作，如读、写标签上的制定存储区。SkyeWare 采用 C 语言的 API(下文有述)。关于 Skyeware 更多信息，请看开发包用户指南。
- SkyeCommand –基于标签类型和选择标记 SkyeCommand 有效的提供了 GUI 接口为了构架 SkyeTek Protocol v3 指令里的 ASCII 或二进制任何一种格式。SkyeCommand 方便您建立、测试低级 SkyeTek 协议指令并充分利用阅读分类功能器的协议层特征。它是更多的学习 SkyeTek Protocol v3 指令的最佳途径。更多信息，请查看开发包用户指南。
- C API – 界于 C 语言和用 SkyeTek Protocol v3 交流的任意 SkyeTek 阅读模块之间的推荐界面。API 提供了丰富的分类功能进入和操作 M9。描述方法可以在 C API 文档中得到，C API 文档在 SkyeWare 安装文件夹中。

第二章

机械规格

M9 模块有装配孔式(MH)和 CF 卡接口两种形式可选。

- 看附录 C 里的"SkyeModule M9 Version 2.0" C-111 页 M9 先前版本的规格说明书。

装配孔式

见第 2-16 页，图 2-1 所示 MH 的尺寸规格

外形尺寸：53.0 mm x 70.0mm = 3710 mm^2
厚度：7.7 mm
安装孔：3.0mm(直径)
两边中心间距 45.0mm
前后中心间距 40.0mm
侧距：孔边缘距印刷电路板(PCB)左右两侧大约 2.5mm (边间距)
孔边缘距印刷电路板(PCB)前侧边缘大约 13.2mm(主连接器端)
孔边缘距印刷电路板(PCB)后侧边缘大约 14.0mm(天线连接端)
重量：17.0 g

注意：所有的图画尺寸都是以毫米计算的。实际生产产品可能会有些许的偏差。

机械规格

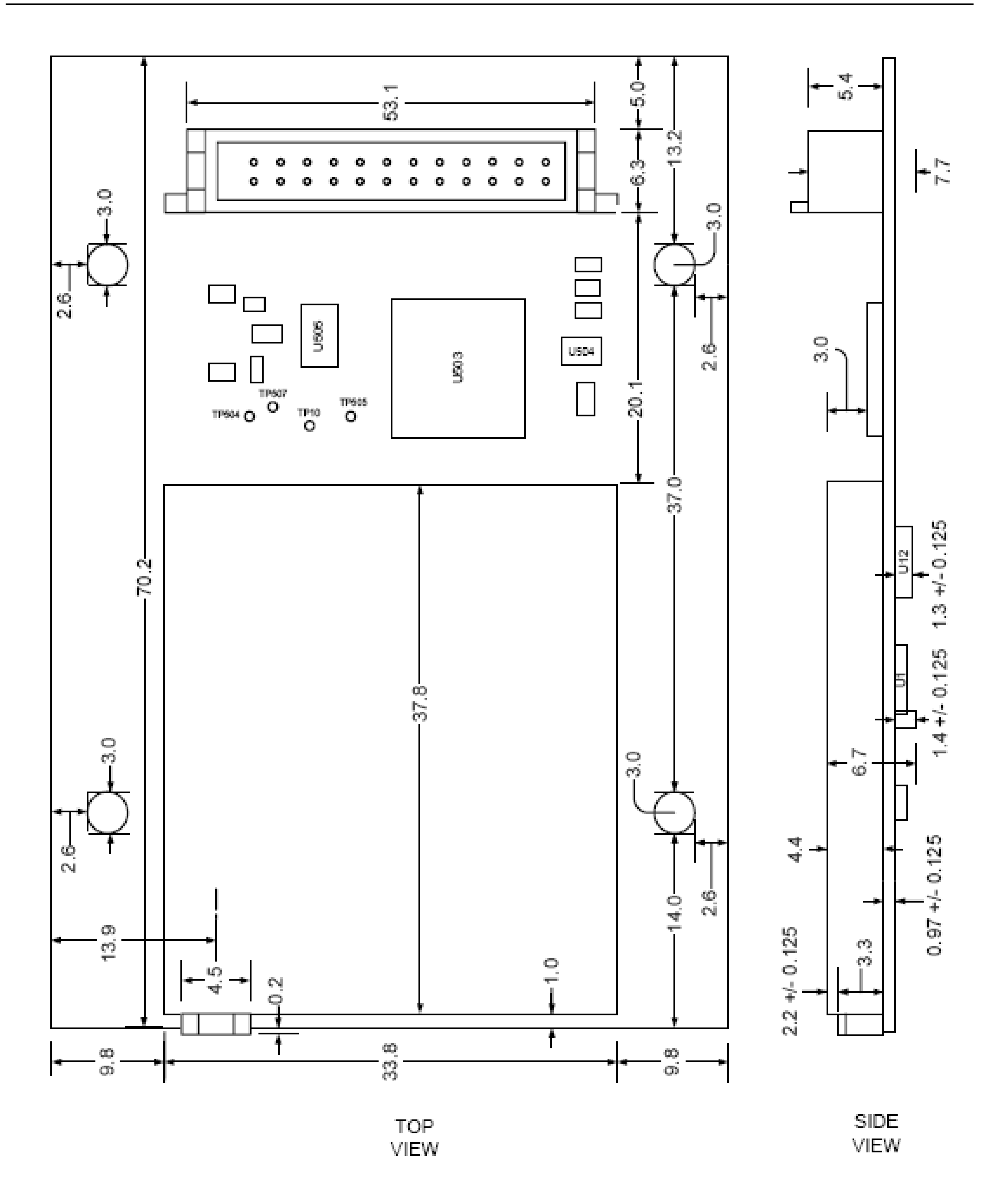


图 2-1 SkyModule M9 Dimensions (MH Variant)

CF 卡式

见第 2-18 页，图 2-2 所示 CF 的尺寸规格

尺寸：66.1 mm x 32.5mm = 2148.25 mm^2

厚度：6.35 mm

重量：14.2 g

注意：所有的图画尺寸都是以毫米计算的。实际生产产品可能会有些许的偏差。

连接器说明

表 2-1 SkyeModule M9 Connector Specifications

模块类型	连接器类型	生产商	生产部编号
M9-CF	CF 类型 II	Molex	67799-0011
M9-MH	插入式电缆母头	Hirose	DF11Z-24DS-2V

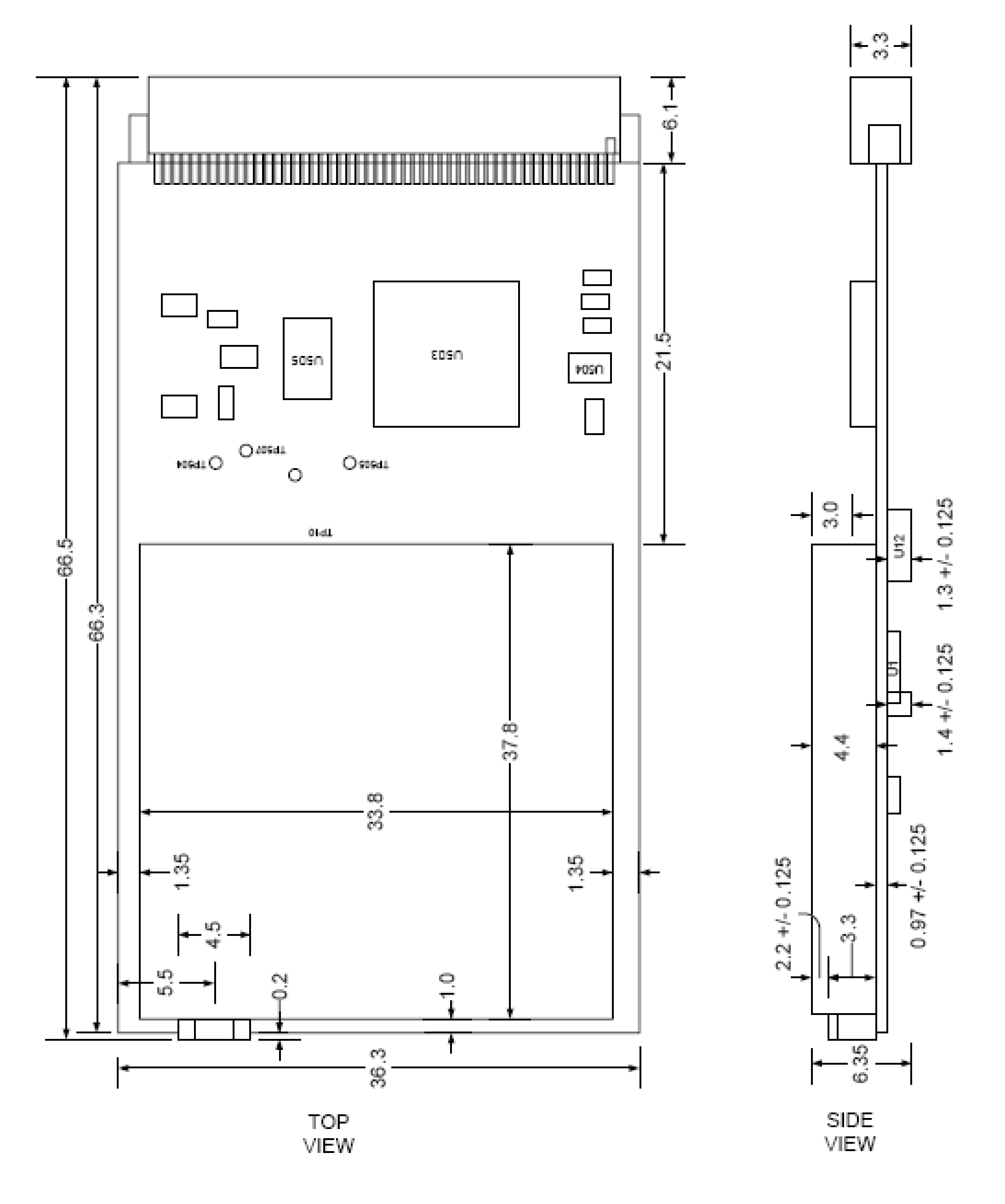


图 2-2 SkyModule M9 Dimensions 尺寸（CF 卡式)

第三章

技术要求说明

注意：看附录 C 里的”SkyeModule M9 Version 2.0” C-111 页 M9 先前版本的规格说明书。

静电警惕

警告 – 如果没有小心预防静电可能会导致 SkyeModule M9 的失败。

M9 模块包含静电敏感器件。请注意遵守以下防范措施防止损坏。

- 当触碰模块时，请佩戴好静电接地手套。
- 保持所有塑料制品，乙烯基和泡沫聚苯乙烯（除抗静电的标明）远离印制电路板。
- 不要用手或者导体去触碰印制电路板上的任何器件或模块。

一般值和运行条件

表 3-1 环境值/运行条件

规格	值
温度范围	温度是 25 摄氏度除非另外说明
运行	-20 到+70 摄氏度
存储	-30 到+85 摄氏度
湿度	
工作，长期存放	10 – 90%（非冷凝态）
暂时存放（<24 小时）	5 – 95%最大（非冷凝态）
ESD 保护	<1kv (ESD HBM 15500 欧姆，100pF) 或 100v (ESD MM 0.75uH,200pF)

第四章

电器规格

这节谈论 M9 模块的电器规格。除非另外说明以下数据将应用于这些规格：

- 温度是 25 摄氏度
- 频率是 915.0MHz
- 供电电压 5V

M9 在符合以下要求的普通环境下,即使全功率输出也无需外接风扇等散热设备,除非一些特殊应用需另处考虑.

注意：请看“静电警惕”3-19 页面的电子安全信息。

表 4-1　M9 电气规格

详述	小	中	大	单位
逻辑输入				
高电压输入	2			V
低电压输入			0.8	V
输入电流		4	25	mA
逻辑输出				
高电压输出(V_{OH})	2.9			V
低电压输出(V_{OL})			0.4	V
输出电流		4	25	mA
供电				
供电电压	3.5	5.0	5.5	V
电流消耗峰值				
10dBm	200		300	mA
21dBm	200		500	mA
24dBm	200		650	mA
27dBm	200		800	mA
睡眠模式		5		mA

绝对最大值:

在没有另行通知的情况下,温度在 25 摄氏度下使用.

表 4-2 绝对最大值/运行条件

规格	值
最大输入电压(V_{INH})	5.5V
供电接地	5.5V
数字输入输出接地	5.5V
天线电压驻波比	优于 2:1 满足具体要求

第五章

主机接口详述

以下章节讲述 M9 电源以及主机接口通信方面的信息.

主机到读写器的通信接口

为了 M9 便于和现有系统的集成,提供了以下微控制主机接口:

TTL (RS232 可以支持额外的电路)

SPI

I^2C

USB

M9 和 Common Blade 系列接口板(CBIB)，支持 RS232 和 USB 通信.主机接口板提供了 USB 接口和 TTL 及 RS-232 到 TTL 的主机接口转换. 主机接口系统参数决定了使用何种接口与主机通信.每种接口通过软件选择完成并且同一时间只允许使用一种接口.主机接口在设置有效功率值和能够被改变的运行时间基础上设置. 在使用 skyeTek Protocol V3 控制主机发送结束的情况下运行 M9

TTL

两根串口线分别是 TXD 和 RXD 连接(没有握手协议).TXD 和 RXD 可以在模块上找到相应的点。根据 SkyeTek Protocol v3（ASCLL 或二进制格式），数据在主机和 M9 进行交换。图 5-1 所示典型的例子。

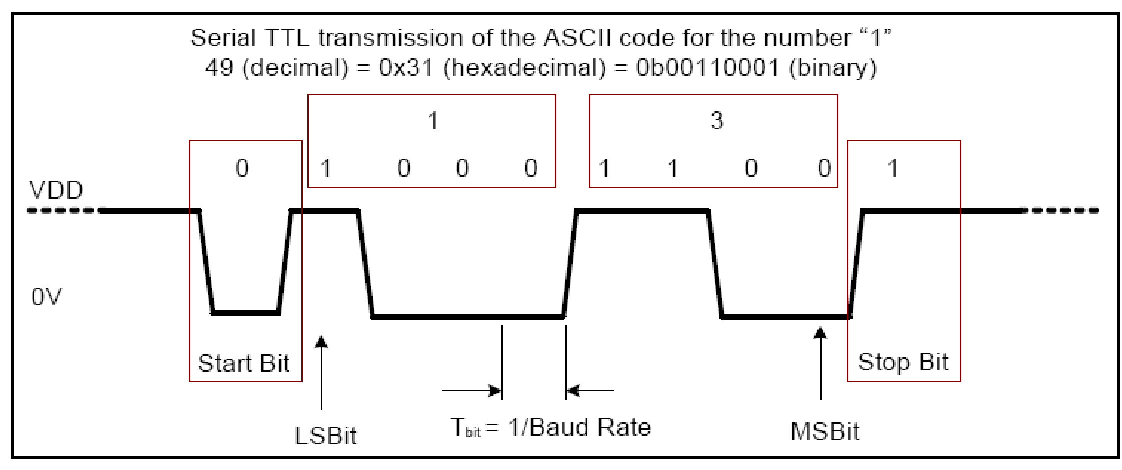


图 5-1 TTL 接口

- 波特率是可选的，通过相应的系统参数来设置，程序出厂默认波特率38，400波特，N，8,1（无奇偶校验，8位数据，1位停止位）。
- 字节通过LSB最低有效位传输，首先通过典型串行数据格式的起始位，然后是8位数据位，最后是1位停止位。
- TTL支持从9600到115200波特的数据传输率，无奇偶校验位，8位数据位，1位停止位。
- 日后还会增加对硬件控制流的支持，目前版本中还未实现。
- 主机到读写器的接口为RS-232TTL方式（不可颠倒）。
- TTL低电压=0-08V;TTL高电压=2.0-5V。

TTL转换RS232

如图5-2 所示连接M9模块无需主机接口板的电路样式。

注意：请确保连接两个供电电压及两个地面线路，以便有足够的电流。否则会导致主机或 M9 模块的损坏和失败。

注释：您可能需要添加额外的迂回电容来减少噪声信号,取决于系统中使用的电路。

注释：skyeytek 建议该电源电路提供 1 安培的电流,以确保正常工作。

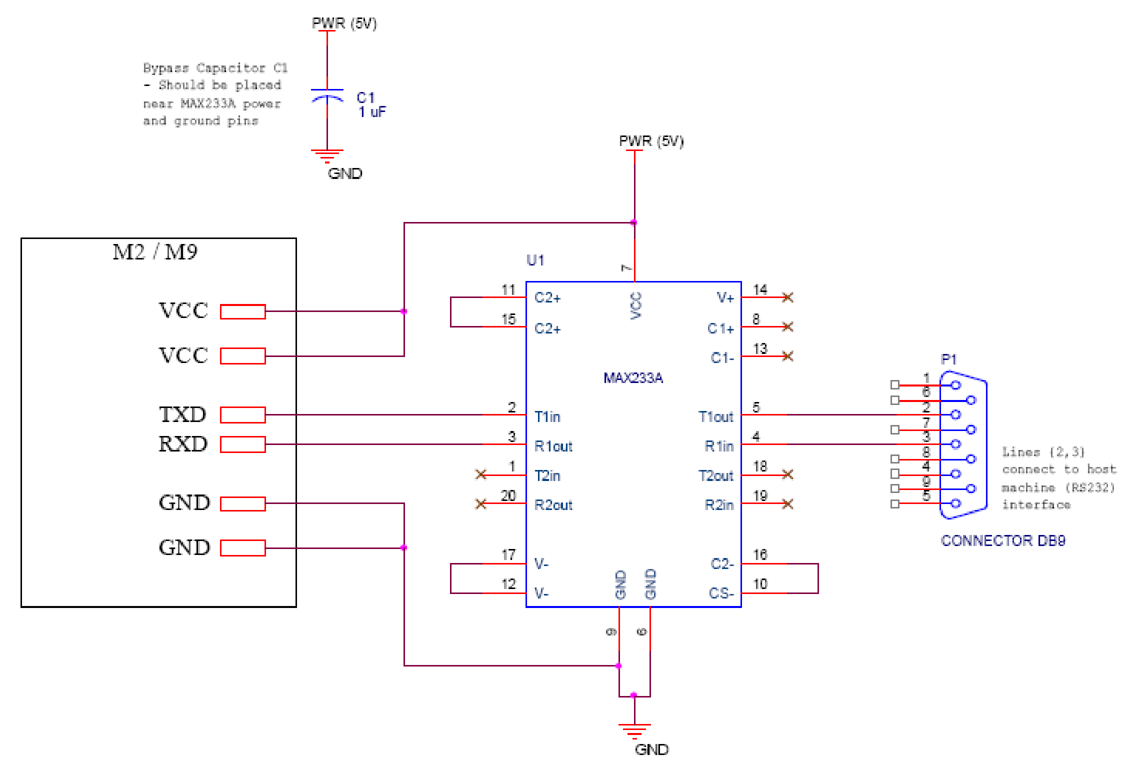


图5-2 TTL转换RS232电路图

SPI

M9具有一个简单的三线SPI主机接口，典型的主机接口通信如下图5-3所示。

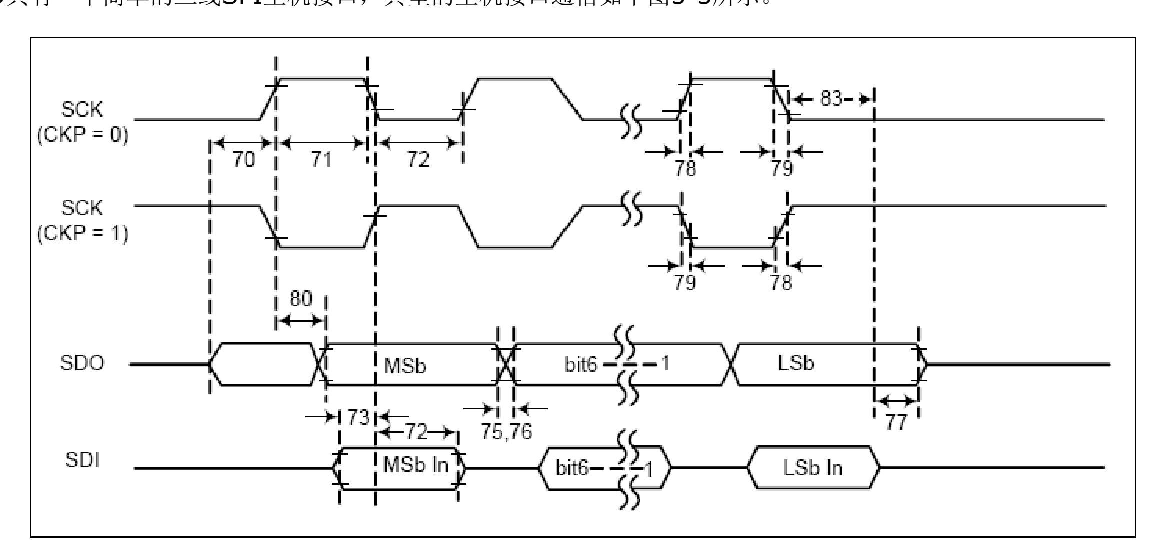


图5-3 SPI接口

- 如果采用该接口,主机须实现 SPI 的主机功能.
- SCK 线为时钟信号,仅由主机控制.
- MOSI(主机输出从机输入)信号从主机向 M9 提供数据.

- MISO(主机输入从出输出)信号从 M9 向主机提供数据.
- SSEL 引出 低态有效.
- 在稳定状态下 SPI 主机软件应设置 SCK 引脚为低电平.
- 数据在 SCK 信号的下降沿传输.
- 与 M9（SPI 从机）之间的数据包交换采用 SkyeTek 第 3 版协议（仅二进制模式）.
- SPI 接口数据传输率可高达 10MHz.
- 当读写器需要向主机发送数据时发出一个等待信号(循环模式或详细目录模式).
- 低电平=0-0.8V 高电平=2.0-5V.

I^2C

M9支持标准I^2C连接到主机控制器。图5-3所示I^2C主机接口连接。

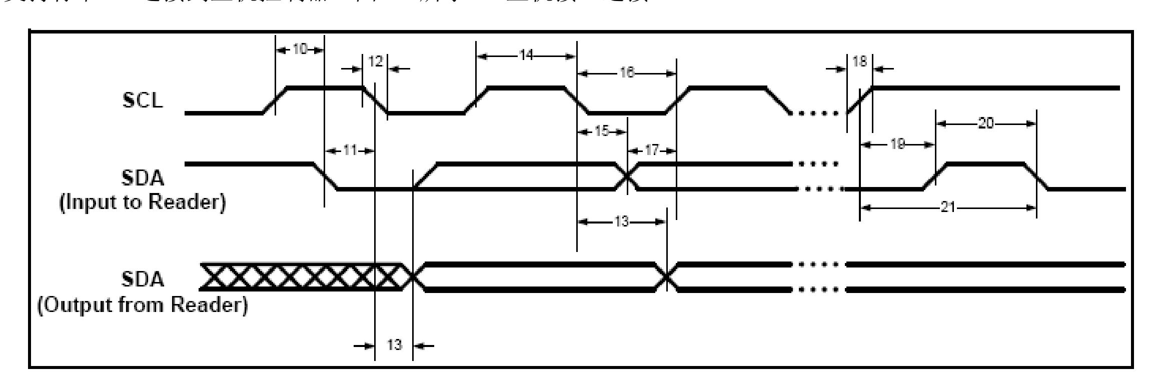


图5-4 I^2C主机接口

- M9 要求主机作为主要的操作（比如，M9 作为I^2C的子设备。）.
- 标准两线连接,是用在 SCL 主时钟和 SDA 一个双向串行数据线.
- 主机与 M9 之间的数据交换采用 SkyeTek 第 3 版协议（仅二进制模式）.
- 快速 I2C 总线模式的支持,提供了 400khz 数据传输率或减慢 100khz 数据传输率.
- 当读写器需要向主机发送数据时发出一个等待信号(循环模式或详细目录模式).
- 数据发送和接收 MSB 为先.
- I^2C拉扯电阻器是在读写器这边.
- 低电平=0-0.8V 高电平=2.0-5V.

USB2.0

USB 被主机识别为一个 HID 设备;
M9 支持全速 USB.

注意：当 M9 为 USB 总线供电时,最大发射功率不得超过 20dBm.M9 配备 SkyeTek 开发包预使用 USB 通讯和功率为 20dbm。

绕过主机接口板

图5-5所示 在没有使用主机接口板的情况下USB通讯电路。

警告：为了防止损坏主机 USB 端口，请确保 M9 模块的功率至少为 20dBm。

注释：您可能需要添加额外的迂回电容来减少噪声信号,取决于系统中使用的电路。

注释：skyeytek 建议该电源电路提供 1 安培的电流,以确保正常工作。

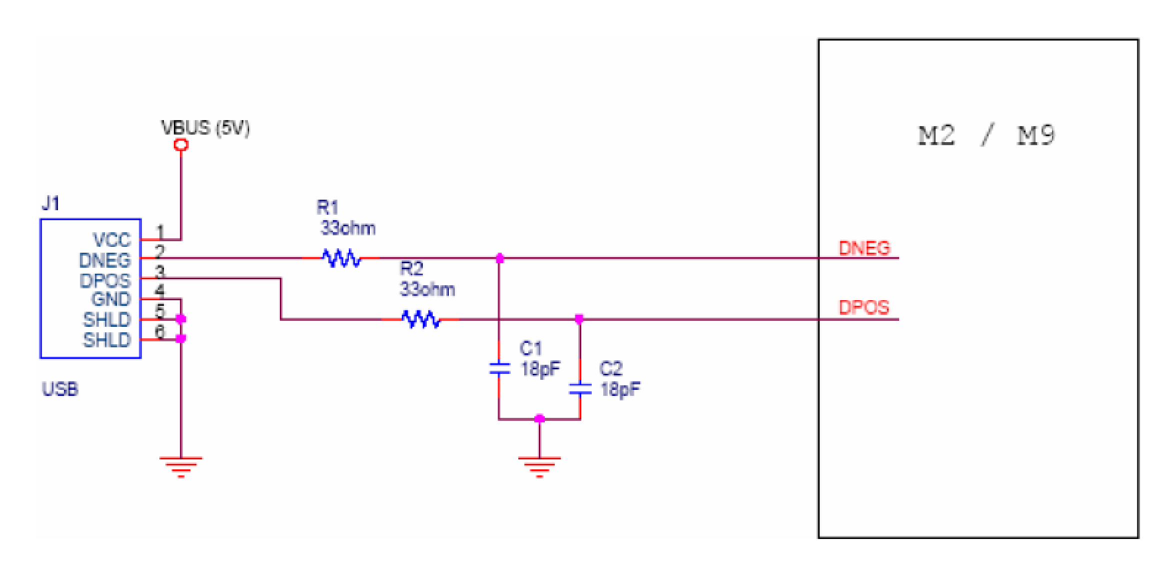


图5-5 电路绕道主机接口板USB支援

M9 接口

这节介绍 M9-MH 和 M9-CF 接口.这些信息将有助于您更好的将 M9 连接到自己电路板或设备中去.

M9-MH引脚详注

标准的M9-MH主机接口是一个标准的24针引脚公头接口。图5-6所示插脚引线位置的接口。

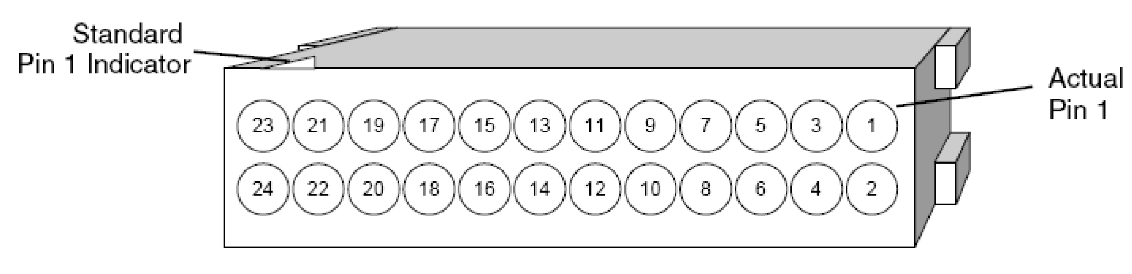


图5-6 M9-MH 接口插脚引线

注意：标准引脚 1 的指标是不符合实际的引脚 1 位置对接头的.引脚 1 是设在同一侧的接头作为指标,但在对面结束排针。（图 5-6）

M9-MH 的引脚信息如 SkyeModule M9 表 5-1 所例:

表5-1 SkyeModule M9-MH 引脚

引脚	名称	描述
1	TXD_ISP	SkyeTek 调试
2	SSEL	SkyeTek 调试
3	RSD_ISP	SkyeTek 调试
4	SCK	SPI 时钟
5	RESET_N	SkyeTek 调试
6	MOSI	Master-out slave-in for SPI
7	NC	没有连接
8	MISO	Master-out slave-in for SPI
9	VCC	电源供电
10	GND	接地
11	DNEG	USB 负
12	SDA	SkyeTek 调试
13	DPOS	USB 正
14	CTS_SCL_HOST	SkyeTek 调试
15	VCC	电源
16	GND	接地
17	GPIO3_MUX	通用 I/O 口，控制 LED 在 U502
18	RTS	SkyeTek 调试
19	GPIO2_7816_IO	通用 I/O 口
20	CTS_SCL_HOST	SkyeTek 调试
21	GPIO1_7816_CLK	通用 I/O 口
22	TXD	UART 传输
23	GPIO0_7816_RST	通用 I/O 口
24	RXD	UART 接收

警告：如果您进行定制集成您的 M9 模块，请确保您连接所有可用功率和引脚接地。否则会促使模块的损坏和减小读

写范围。

SkyeModule M9-CF引脚详注

M9-CF 通信接口为标准 50 针引脚的 CF(f)接口.引脚输出图 5-7 所示:

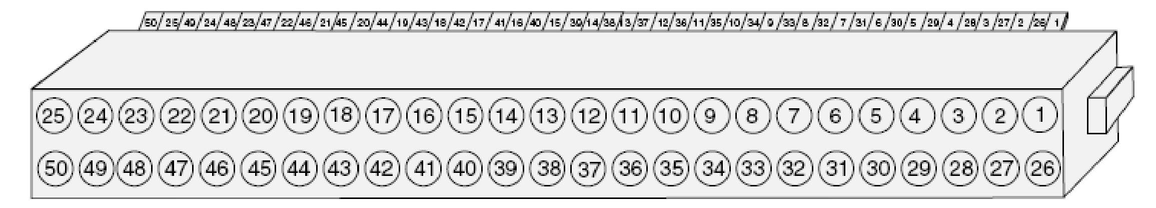


图5-7 M9 CF 输出引脚

针 1 位于突起的左边,箭头在 M9-CF 板的顶上(针脚 1 边上突起的顶上的箭头的位置).见图 5-8:

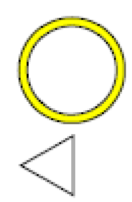


图5-8 引脚1边上突起顶上箭头的位置

表 5-2 SkyeModule M9 所列为 M9-CF 接口引脚的含义.(所有没有连接的脚可以闲置)

表5-2 SkyeModule M9-CF 插脚引线

引脚	名称	描述
1	GND	接地
2	VCC	供电电源
3	VCC	供电电源
4	DPOS	USB 正
5	DNEG	USB 负
6	GND	接地
7	MISO	主机输入,从机输出 对 SPI
8	MOSI	主机输出,从机输入 对 SPI
9	SSEL	SPI 从机选择
10	SCK	SPI 时钟
11	SCL_EEPROM	SkyeTek 调试
12	SDA_EEPROM	SkyeTek 调试
13	NC	没有连接
14	RXD	通用异步收发接收
15	TXD	通用异步收发发送
16	CTS_SCL_HOST	SkyeTek 调试

17	RTS	SkyeTek 调试
18	NC	未连接
19	TRST_N	SkyeTek 调试
20	RTCK	SkyeTek 调试
21	TMS	SkyeTek 调试
22	TCK	SkyeTek 调试
23	TDI	SkyeTek 调试
24	TDO	SkyeTek 调试
25	GND	接地
26	GND	接地
27	GND	接地
28	CTS_SCL_HOST	SkyeTek 调试
29	SDA_HOST	SkyeTek 调试
30	NC	未连接
31	NC	未连接
32	GPIO0_7816_RST	多种用途的 I/O
33	GPIO1_7816_CLK	多种用途的 I/O
34	GPIO2_7816_IO	多种用途的 I/O
35	TXD_ISP	SkyeTek 调试
36	RXD_ISP	SkyeTek 调试
37	NC	未连接
38	NC	未连接
39	NC	未连接
40	READY_N	SkyeTek 调试
41	RESET_N	SkyeTek 调试
42	NC	未连接
43	GPIO3_MUX_EN	外接 I/O 口
44	GPIO4_MUX_CNTRL2	外接 I/O 口
45	GPIO5_MUX_CNTRL1	外接 I/O 口
46	GPIO6_MUX_CNTRL0	外接 I/O 口
47	NC	未连接
48	NC	未连接

49	GND	接地
50	NC	未连接

警告：如果您进行定制集成您的 M9 模块，请确保您连接所有可用功率和引脚接地。否则会促使模块的损坏和减小读写范围。

第六章

射频规格和区域遵守

射频功率

M9 的射频传输功率可以由用户在 -20 到 +70 摄氏度的温度范围内以 0.1dB 为单位的步进值进行调整，精度为 +/-1 dB，范围为10-27dBm，从而得以降低功耗，满足一些系统的低功耗要求。由于调整的最小步进值的解析度要大于精度值，因此可以通过细调功率水平而降低电流消耗。关于如何调整射频功率大小，请参阅第10章节"系统参数"。

频率

M9是一个可以在862-955MHz范围内工作的多频段设备，几乎涵盖了世界上所有主流UHF市场的频段。关于如何调整M9的工作频率和区域选项，请参阅"调节系统参数"。

标签协议

M9支持对以下标签进行基本处理命令（识别，读操作，写操作）：

- EPC C1G1
- EPC C1G2(ISO18000-6C)
- ISO 18000-6B

注意：此表所列包含 SkyeTek 的 M9 模块目前支持和以后将要支持的标签芯片。更多的当前支持的标签与特征，请详见随机附带 CD 中包含的"标签支持列表"。

各地区的推荐设置

以下设置建议,以帮助您获取调整的认证

表6-1各地区应用设置

地区	起始频率 (MHz)	中心频率 (MHz)	终止频率 (MHz)	输出功率 (dBm)	跳频步长 (KHz)	调制深度 (%)	跳频方式	调整模式	支持标签类型
澳大利亚/新西兰	918.3	922.0	925.7	25	200	100	0x01	0x00	all
欧洲	865.7	866.7	867.9	26	200	30	0x00	ox01	ISO18000-6B
欧洲	865.7	866.7	867.9	22	200	80	0x00	0x01	Gen2
香港	920.3	920.5	924.7	27	200	100	0x01	0x00	all
日本(户内)	952.2	953.0	953.8	22	200	80	0x00	0x02	All
日本(户外)	952.2	953.0	953.8	10	200	80	0x00	0x03	all
韩国	910.3	912.0	913.7	27	200	100	0x01	0x00	all
北美	902.3	915.0	927.7	27	200	100	0x01	0x00	all
新加坡	923.3	924.0	924.7	27	200	100	0x01	0x00	all
台湾	922.3	925.0	927.7	27	200	100	0x01	0x00	all

a. 更多现有列表支持的标签和特征，请看标签支持列表。其包含在随 CD 安装的文件夹文档里，或看 Skyetek 支持协议。

b. 日本的调制模式采取用 Skyetek 外加的日本区域过滤. 过滤介绍损失 1-2db 信号强度和当设定其中的一个日本调制模式时,SkyeModule 固件可以弥补这方面的损失。

区域调整

表6-2 SkyeModule M9通过认证

地区	机构	认证	备注
北美	FCC	Part 15 standards	
欧洲	ETSI	EN 301-489	“Electromagnetic and Radio Spectrum matters (ERM); Electromagnetic Compatibility (EMC); standard for radio equipment and services; Part 1: Common technical requirements”
		EN 61000-4-3	“Radio Frequency Electromagnetic Field”

		EN 302-208	“Electromagnetic Compatibility and Radio Spectrum Matters (ERM): Radio Frequency Identification equipment operating in the band 865 MHz with power levels up to 2 W: Part 2 Harmonized EN under article 3.2 of the R&TTE directive”
台湾		LP002	“Low Power Radio Frequency devices”
香港		HKTA 1049	“Performance Specification for Radio Frequency Identification (RFID) Equipment Operating in the 865-868 and/or 920-925 MHz bands”
韩国	Radio Research Laboratory	Notification No. 2005-50	“Technical Requirements for the Radio Equipment for Other Services than Broadcasting, Maritime, Aeronautical and Telecommunications Service”
新加坡		IDA TS SRD	
澳大利亚		AS/NZS 4268:2003	“Radio equipment and systems – Short range devices – Limits and methods of measurement”

射频规格

分类	小	中	大	单位
RF特性				
频率范围 (直接输出)	862.000	915.000	955.000	MHz
跳频步长	100	200	300	KHz
发送参数				
发射功率	10	12	20/27*	dBm (详见附录A1中的各地区最大功率标准信息) 当M9处于USB供电时，最大功率为20dBm
不同温度下发射功率变化		+/-1		dB(温度范围:-10C - +55C)
不同电压下发射功率变化		+/-1		dB(VCC范围:3.5V – 5V)
不同频率下发射功率变化		+/-1		dB(频率范围:862-955MHz)
最适宜外接负载阻抗		50		Ohms
接受参数				
灵敏度	45	50	55	dBm(发射功率为27dBm) 标准860-960MHz
灵敏度	40	45	50	dBm(发射功率为27dBm) 标准860-960MHz

第七章

天线

M9支持任何适当频率的50 Ohm阻抗天线，具体根据用户需求来定。阅读距离取决于所选定的天线和具体应用环境。

阅读距离与您的详细配置有关，其包括：

- 周围环境：（为了测试的精确性和得到最佳化，SkyeTek建议您在户外空地进行测试。）
- 天线增益：（高增益天线提供了较长的读写范围，然而，这个射程是通过一个较小的波束宽度,从而减少了读写领域,影响读写可靠性。）
- 天线电缆长度：（天线电缆增益/损耗约为-0.49db/米(-0.15db/英尺)标准RG58同轴电缆。）
- 射频功率：最大射频功率为27dBm。
- 跳频设定：（取决于天线）
- 天线的极化
- 标签的倾向性
- 标签的类型，厂商，个别标签
- 标签的芯片
- 标签的动态(速度，移动，旋转)

第八章

软件规格

主机通信-SkyeTek v3协议

M9 的操作方式遵循 SkyeTek 协议第三版。有关此协议的更多信息。包括命令，标识符，请求及响应格式请参照 SkyeTek 协议第三版参考指南。

基本的格式命令与响应时间遵循以下说明。

表8-1 请求格式(bytes), ASCI I格式

标识符	命令	读头ID	标签类型	标签ID Len	标签ID	AFI	地址	#of Bloks	数据长度	数据	奇偶校验
4	4	8	4	4	32 (max)	2	4	4	4	2K	4

表8-2 请求格式(bytes), 二进制格式

信息长度	标识符	命令	读头ID	标签类型	标签ID Len.	标签ID	AFI	地址	#of Bloks.	数据长度	数据	奇偶校验
2	2	2	4	2	1	16 (max)	1	2	2	2	1K	2

(深灰)	必要部分(每条命令必须包含该部分)
(浅灰)	选择区域(根据命令与标识符)
(白)	必要区域(根据命令)

表8-3 响应格式(bytes), ASCII 格式

响应字符	读头ID	标签类型	数据长度	响应数据	奇偶校验
4	8	4	4	2K	4

表8-4 响应格式(bytes), 二进制格式

数据长度	响应字符	读头ID	标签类型	数据长度	响应数据	奇偶校验
2	2	4	2	2	1K	2

(深灰)	必要部分(每条命令必须包含该部分)
(浅灰)	选择区域(根据命令与标识符)
(白)	必要区域(根据命令)

SkyeSuite™ 开发软件

所有 SkyeModule M9 开发包包含以下部分工具软件:

- C API - C 语言 API 提供 C 程序语言和任意 Skyetek 模块之间利用 Skyetek 协议第三版的通信接口。C-API 提供了大量基于讯问控制 M2 阅读模块的功能函数。在 C-API 文档中还包含了这些算法的函数。

- SkyeWare - SkyeWare 是一个用来连接,配置,升级 SkyeTek 模块的窗口化控件，也可以通过它来演示标签的基本操作，如搜索特定区域的所有标签，以及对标签的读/写和加密操作.SkyeWare 同样是使用 C API。需要更多有关 SkyeWare 的信息，请看 SkyeWare 用户指南。

- Skye Command Builder - 命令编辑器是一个窗口化控件工具，用来编辑符合 SkyeTek 协议的命令并返回符合 SkyeTek 协议的响应信息。用户可以通过该控件编辑简单命令并调用所有模块的协议级功能。有关更多该工具的信息。请参照命令编辑器(Skye Command Builder)。

对于这个话题的更多信息，请看开发包用户指南。

第九章

使用安全存贮器

注意：使用安全存贮器功能需要指定一个具体 M9 固件版本。请联系 SkyeTek 的销售部索取一个正确的固件。

作为Readerware安全套件的一部分,安全存贮器使用SkyeModule M9的固件，把加密功能添加到RFID标签里，此方法通常没有集成安全机制。具体来说，安全存贮器允许数据被写入射频识别标签后进行签署，加密，或两者即可。M9支持多种加密算法（DES,3DES 和 AES）和多种散列函数（SHA,MD5,和SHA-224/256/384/512）来签署或验证信息的真实性和完整性。

M9会在标签存储上保存有一些算法信息，初始化变量和密码。当您使用安全存贮器时，M9会确保对待整个标签存储数据的安全，用户不需要去阻止。

签署您核实数据的真实性和完整性。读写器在纯文本和加密文本上增加一个哈西值，将其和读写器信息储存在标签上。通过计算哈西值，使用知名的共享密钥和纯文本 并通过校检结果反向增加哈西值。这样您可以确认信息被授权用户发出或终止，即终止数据在传输中被损坏或纂改。

无论信息发出或存储在标签里，加密可以像遮蔽信息一样让你隐藏纯文本数据。只有授权的用户持有正确的密码才可以进行解密。

这一章节提供些使用安全存储器命令的例子。更多有关Readerware安全组件资料，请联系SkyeTek。

使用安全存储器命令

一旦被启动，所有安全操作处理以下命令：

- 读标签数据
- 写标签数据
- 获得标签信息

以下是两种主要的操作模式：

- 完整数据模式

这种模式没有编译码，但读写器验证数据的完整性。当写数据到标签的时候，读写器自动处理数据的安全。读写器会写数据和信息授权码（HMAC）到标签。当读标签返回数据时，读写器会验证数据开始写入标签时HMAC的匹配性。如果检测到HMAC不匹配，说明数据已经被纂改或损坏，读写器返回给主机一条失败的信息。

- 加密盒完整数据模式

这种模式，读写器验证数据完整性和加密的数据。读写器写入加密数据和HMAC到标签。当读从标签返回到数据时，读写器会验证数据开始写入标签时HMAC的匹配性，译解数据和一个以纯文本数据返回给主机。如果数据被纂改，读写器返回一条失败的信息给主机。

安全存储器注意事项：

- 在您开始使用安全存储器之后，必须使用带有HMAC和加密标识符的命令。
- 安全存储器会为安全使用自动重定格式标签。这样，区块0在安全存储器模式不能通信到区块0的物理存储标签。在标签运算和关键信息之初，初始化安全存储器命令自动储存许多区块。命令同样可以调整标签储存大小，提供一个新的用户储存大小给标签，此时初始化用户储存区域为0。例如，如果您在数据初始化模式写入区块0，您不能从标签物理区块0位置读回纯文本信息。

- 如果你尝试读一个已被初始化或文本加密和读写器的数据完整性模式的安全存储器标签的内容，那是非安全存储器模式。您将看到加密文本或初始化信息，取决于您从哪个区块读取。

- 如果你读一个已被初始化或文本加密和读写器的数据完整性模式的安全存储器标签的内容，那是安全存储器模式，您可以读取纯文本数据（只要标签数据尚未被纂改和损害）。

- 读和写命令是用来读写安全存储器的一旦安全存储期已初始化。读和写命令应该看作通常的读写命令一样读取非安全存储器模式标签，除此标识符必须被指定和应该被指定了的HMAC_F，如果HMAC已用和应该指定加密的ENC_F。

- 在您开始使用安全存储器标签之后，标签存储大小会出现改变。在正常运作时,获得标签信息命令返回物理内存布局标签。在安全存储器模式，获得标签信息命令返回起始区块,最大区块和一些区块的重定格式,并能够利用用户存储器。

- 您可以通过取消选择初始化标签来停止使用安全存储其功能，可以重新选择标签没有标识符设定。

选择安全算法

安全存储器可以让您选择算法来计算哈西消息授权码（HMAC）用数据完整性模式或加密数据完整性模式都可以。（表9-1）

- 数据完整性模式下您可以选择表格里的任何一种。

- 加密数据完整性模式，您可以使用任何一种哈西和任何一种密码。

表9-1 SkyeTek ReaderWare 安全算法

Function:	**Algorithm:**	**Options/Notes:**
Cipher	TDEA (Triple-DES)	Key Sizes: 56, 112 and 168 bits
		Modes: ECB, CBC, CTR
	AES (Rijndael)	Key Sizes: 128, 192 and 256 bits
		Modes: ECB, CBC, CTR
Hash	SHA-1	Modes: Iterative, One Pass
	SHA-224	Modes: Iterative, One Pass
	SHA-256	Modes: Iterative, One Pass
	SHA-384	Modes: Iterative, One Pass
	SHA-512	Modes: Iterative, One Pass
	MD5	Modes: Iterative, One Pass
HMAC (keyed hash message authentication code)		
	HMAC	Hashes: All available
		Modes: Iterative, One Pass
PRNG (pseudo random number generator)		
	SHA1PRNG	

- 由于空间的协定,并非所有支持的标签支持所有算法选择。在启动安全存储其之后，确保了标签上还有多少可用空间。
- 当您使用SkyeTek的ReadWare(上表9-1)任一支持的密码格式时，安全存储器总是使用密码计算器（CTR）模式。这种模式提供了加密系统性能让安全存储器使用全部标签内存无需为区块填料和凑整。又可让安全存储器升级标签唯一一部分取代重写整个标签。这不可能以密码区块链接（CBC）或电子代码薄方式同样用于每一个密码。

安全级别的算法匹配

当可能时，您应该根据可比较的安全级别配对算法。安全级别描述攻击算法期望的难度。例如，一个安全级别为80意为着要执行2^{80}要求才能够破解此算法。新应用程序不应该使用低于80以下的算法与安全级别。以下表格列出了安全级别的可用算法。

表9-2 安全级别

Security Level	Algorithms
< 64 (legacy applications only)	TDEA-56, MD5
80	SHA-1, TDEA-112
112	SHA-224, TDEA-168
128	AES-128, SHA-256, SHA1PRNG
192	AES-192, SHA-384
256	AES-256, SHA-512

使用密钥导出函数增强安全性

您也可以使用安全存储器的一个密钥导出函数（KDF）。启用其函数时，KDF使用您指定的密钥申请一个HMAC，标签ID和应用类型得出一个特殊标签和特殊用途密钥在您设置或初始化安全存储器之前。使用KDF可以增强您用安全存储器建立应用的安全：即使强力攻击成功一个单独标记，它不减弱用于多个标记的万能密钥。

要使用KDF，使usekeyderivationfunc标识符在ASN1.BER编码数据为初始化安全存储器或设定安全存储器命令。

初始化安全存储器（**0x0203**）

初始化安全存储器命令用安全存储器特征设定一个支持存储器标签。它设置所有算法和模式设置，然后初始化标签安全数据到零置状态。随后应该参考设置安全存储器命令来使用初始化安全存储器标签（请看9-55页”设置安全存储器(0x0204)”）。

- 此命令要求您首先为标签创建一个情形。
- 请求和返回数据域在数据域格式使用ASN.1 BER编码，如指定，虽然您不需要使用ASN.1 BER标准知识的命令。

在SkyeTek协议信息的“数据”部分应递送这些模板例子。

数据邻域格式（**ASN.1BER 编码**）

为初始化安全存储器，在SkyeTek协议命令的“数据”部分应递送这些信息。

Request

```
SEQUENCE {
   macAlgorithm            ENUMERATED {
   HMAC-SHA1(1), HMAC-SHA224(2), HMAC-SHA256(3),
   HMAC-SHA384(4), HMAC-SHA512(5), HMAC-MD5(6)
    },
  macKeyName          [1] OCTET STRING OPTIONAL,
  macKey                  OCTET STRING,
  cipherAlgorithm         ENUMERATED OPTIONAL {
    TDEA-56(18), TDEA-112(34), TDEA-168(66),
    AES-128(49), AES-192(81), AES-256(97)
  },
  cipherKeyName       [2] OCTET STRING OPTIONAL,
  cipherKey               OCTET STRING OPTIONAL,
  useKeyDerivationFunc    BOOLEAN OPTIONAL
}
```

Response

(There is no response data.)

例 – 初始化安全存储器（只适合数据完整性）

初始化数据完整模式，使用HMAC-SHA1：

请求

30800A01**01**04_20_**FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF**
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFF0000

- 开头粗体部分是HMAC算法标识符（01为HMAC-SHA1）

Identifier	Algorithm
1	HMAC-SHA1
2	HMAC-SHA224
3	HMAC-SHA256
4	HMAC-SHA384
5	HMAC-SHA512
6	HMAC-MD5

- 开头斜体部分（20）是HMAC密钥长度
- 后面粗体部分为HMAC密钥

返回

（无数据返回）

例 – 初始化安全存储器（加密和数据完整性）

设置加密和数据完整性模式，用AES128和HMAC-SHA1:

请求

30800A0101042*0***FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF**
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFF0A0131042*0***FFFFFFFF**
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFF0000

- 开头部分粗体为HMAC算法标识符（01为HMAC-SHA1）
- 开头部分斜体是随后HMAC钥匙的长度
- 第二部分粗体为HMAC密钥
- 指定各自密码算法标识符和密码索引。中间斜体部分指定随后密码索引。
- 第三部分粗体部分是密码算法标识符

Identifier	Cipher
18	TDEA-56
34	TDEA-112
66	TDEA-168
49	AES-128
81	AES-192
97	AES-256

- 第二部分斜体部分指定随后密码索引
- 结尾部分粗体为密码索引

返回
（无数据返回）

设置安全存储器（0x0204）

设定安全存储器命令改变已经初始化了供安全存储器使用的存储器标签。（请看9-52页"初始化安全存储器"(0x0203)）

- 此命令要求您首先为标签创建一个情形。
- 请求和返回数据域在数据域格式使用ASN.1 BER编码，如指定，虽然您不需要使用ASN.1 BER标准知识的命令。

ASN.1 命令数据的描述

为初始化安全存储器，在SkyeTek协议命令的"数据"部分应递送这些信息。

请求

```
SEQUENCE {
  macKeyName          [1] OCTET STRING OPTIONAL,
  macKey                  OCTET STRING,
  cipherKeyName       [2] OCTET STRING OPTIONAL,
  cipherKey               OCTET STRING OPTIONAL
  useKeyDerivationFunc    BOOLEAN OPTIONAL
}
```

返回

（无数据返回）

例 – 改变数据完整性字符串（只适合数据完整性）

请求

08004*20***FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF**
FFFFFFFFFFFFFFFFFFFFFFF0000

- 斜体部分（20）是HMAC密钥长度
- 粗体部分为HMAC密钥

返回
（无数据返回）

例 – 改变加密术及数据完整性设置

使用加密术和数据完整性，用AES128和HMAC-SHA1:

请求

308004*20***FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF**
FFFFFFFFFFFFFFFFFFFFFFFF04*20***FFFFFFFFFFFFFFFFFFFF**
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF0000

- 第一部分斜体（20）是HMAC密钥长度
- 第一部分粗体为HMAC密钥
- 第二部分斜体是密码索引长度
- 第二部分粗体是密码索引

返回

（无数据返回）

第十章

系统参数

系统参数用于配置读写器设置。可以通过以下命令来访问：

- ReadSystem （从指定地址读出系统当前参数值）
- WriteSystem （按指定地址写入一个新的系统参数值）
- StoreDefaultSystemParameter （将新的系统参数值写入 EEPROM）
- RetrieveDefaultSystemParameter （从 EEPROM 的指定地址中读出系统参数值）

默认设置将在断电或重启后生效。

警告：当读写器重新设置的时候您尚未将数据写入到 EEPROM，任何更改系统参数的信息将会丢失。

表10-1 SkyeModule M9 系统参数

系统参数	参数地址	字节长度(比特)	初始值
串口号	0x0000	4	0x00000000
固件版本	0x0001	4	0xXXXXXXXX 根据所发行的版本
硬件版本	0x0002	4	0xXXXXXXXX 根据所发行的版本
产品号	0x0003	2	0x0009
读头 ID	0x0004	4	0xFFFFFFFF
读头名称	0x0005	32	M9(十六进制)
主机接口类型	0x0006	1	0x00(TTL)
主机接口波特率	0x0007	1	0x02(38400)
用户端口方向	0x0008	1	0x00
用户端口值	0x0009	1	0x00

MUX 控制	0x000A	1	0x00
操作模式	0x000C	1	0x00
命令 Retry	0x0011	1	0x05
功率等级	0x0012	1	0xDC(27dBm)
当前频率	0x0030	4	0x3689CAC0(915Mhz)
起始频率	0x0031	4	0x35C80160(902.3Mhz)
终止频率	0x0032	4	0x374B9420(927.7Mhz)
Hop Channel Spacing	0x0034	4	0x00030D40(200KHz)
Frequency Hopping Sequence	0x0035	1	0x01(pseudo-random)
调试深度	0x0036	1	0x64(100%)
正常模式	0x0037	1	Ox00
LBT 天线增益	0x0038	1	0x00

系统参数描述

此章节介绍每个SkyeModule M9 的系统参数。例子请看"系统参数格式"10-72页。

序列号

- 返回读写器序列号
- 参数地址：0x0000
- 长度（Bytes）：1
- 出厂设置：0x00000000
- 只读

固件版本

- 返回读写器当前固件版本号
- 参数地址：0x0001
- 长度（Bytes）：4
- 出厂设置：0xXXXXXXXX（取决于版本）
- 固件版本使用以下格式：
- 主版本号（1 Byte）
- 副版本号（1 Byte）
- 当前构建号（2 Bytes）
- 只读

硬件版本

- 返回读写器当前的硬件版本
- 参数地址：0x0002
- 长度（Bytes）：4

- 出厂设置：0xXXXXXXXX（取决于版本）
- 硬件版本使用以下格式：
- 主版本号（1 Byte）
- 副版本号（1 Byte）
- 当前构建号（2 Bytes）
- 只读

产品编码

- 返回SkyeTek产品编号（每一个SkyeTek产品都有一个唯一的产品编号。）
- 参数地址：0x0003
- 长度（Bytes）：2
- 初始值：0x0009
- 只读

读写器ID

- 指定的参数Reader ID用来存放标注读写器的标识信息,使读写器只对被指定的指令进行执行与响应。读写器会判断指令中读写器号是否和参数中存放的相同,如果不相同则不做出任何响应。
- 参数地址：0x0004
- 长度（Bytes）：4
- 出厂设置：0xFFFFFFFF（取决于版本）
- 在请求指令中指定RID标记即可启用ReaderID功能,用于多个读写器在同一辆巴士或网状结构工作的情况。
- 读/写

读写器名称

- 用户可自定义一个用32字节长度的读写器名称
- 参数地址：0x0005
- 长度（Bytes）：32
- 初始值："SkyeModule M9"
- 读/写

主机接口类型

- 指定主机通讯接口方式
- 参数地址：0x0006
- 长度（Bytes）：1
- 初始值：0x00（TTL）
- 读/写
- 有效的主机接口值为：
    - 0x00 - TTL
    - 0x01 - TTL Serial
    - 0x02 - SPI
    - 0x04 - I2C
    - 0x06 - USB
    - 其余参数都无效,继续使用当前主机接口。

注意：SkyeTek M9 为了使用 USB 通讯预先配备 SkyeTek 开发包。

主机接口波特率

- 从主机接口设置波特率
- 参数地址：0x0007
- 长度（Bytes）：1
- 初始值：0x02（38400）
- 只在TTL方式下工作
- 只能写
- 有效波特率值为：
    - ox01 - 19,200
    - ox02 - 38,400
    - ox03 - 57,600
    - ox04 - 115,200
    - 除此以外输入任何参数系统默认为9600。

注意：固件的升级您可能需要限制波特率为 38,400。

用户端口方向

- 通过读写器 GPIO 针设置方向
- 参数地址：0x0008
- 长度（Bytes）：1
- 初始值：0x00
- 计数位"1"表示正在使用的 GPIO 为输入信息
- 读数位"0"表示正在使用的 GPIO 为输出信息
- 读/写
- 引脚的相应定义为:
    - BIT0-GPIO0
    - BIT1-GPIO1
    - BIT2-GPIO2
    - BIT3-GPIO3
    - BIT4-GPIO4
    - BIT5-GPIO5
    - BIT6-GPIO6
    - BIT7-RFU

用户端口值

- 通过读写器 GPIO 设置端口值
- 参数地址：0x0009
- 长度（Bytes）：1
- 初始值：0x00

- 计数位"1"表示正在使用的 GPIO 引脚为逻辑高电平
- 计数位"0"表示正在使用的 GPIO 引脚为逻辑低电平
- Enable bit(bit7)设置后才生效
- 可读/可写
- 引脚的相应定义为:
    - BIT0-GPIO0
    - BIT1-GPIO1
    - BIT2-GPIO2
    - BIT3-GPIO3
    - BIT4-GPIO4
    - BIT5-GPIO5
    - BIT6-GPIO6
    - BIT7-Enable

MUX 控制

- 控制 SkyeTek 多路复用。有关 MUX 更多信息请参阅 skyeplus 多路复用器参考指南。
- 参数地址：0x000A
- 长度（Bytes）：1
- 初始值：0x00
- 读/写

工作模式

- 设置为睡眠模式
- 参数地址：0x000C
- 长度（Bytes）：1
- 初始值：0x00
- 向系统参数输入 ox01 使读写器进入睡眠模式
- 在任意接口发送任意指令使模块唤醒
- 读/写

重发指令

- 一个字节
- 系统参数：0x0011
- 长度（Bytes）：1
- 初始值：0x05
- 可以由主机设置
- 在返回一个失败的消息之前，读写器内部执行一个标签命令以记录次数。
- 只适用于标签指定的 SkyeTek 协议命令
- 有效范围为 0-255（0x00-0xFF）
- 在成功响应出现前，命令内部重复”n”次数，n 是主机指定的一个值。当一个成功的反应发生时，读写器停止重复命令并且发送成功反应回到主机。
- 可读/可写

发射功率

- 通过读写器配置功率
- 参数地址:（0x0012）
- 长度（Bytes）：1
- 初始值：0xDC（27dBm）
- 功率在 5dBm-27dBm 之间以 0.1dBm 为精度进行调节
- 写入一个从 50-220 的十六进制数来指定功率值（看表 10-2）
- 通过方程式计算出期望的功率所对应的系统参数值
  （期望功率值 dBm-5)/0.1=相应的系统参数值）

表 10-2 功率参数值

功率(dBm)	SkyeTek 十进制值	十六进制参数值
10	50	0x32
12	70	0x46
15	100	0x64
17	120	0x78
20	150	0x96
21	160	0xA0
24	190	0xBE
27	220	0xDC

- 读/写

当前使用频率

- 用来设置读写器读写标签的频率
- 参数地址：0x0030
- 长度（Bytes）：4
- 初始值：0x3689CAC0(915MHz)
- 通过写入一个 4 字节十六进制参数值调整到相应的期望功率.所需频率和对应的十六进制数参数值请见频率参数值对照表 10-3
- 读/写

注:希望定频的用户只需将当前工作频率.调节最小值及最大值设定成相同的值即可

起始频率

- 设置读写器工作频率的下限
- 参数地址：0x0031
- 长度（Bytes）：4
- 初始值：0x35C80160（902.3MHz）
- 定入一个 4 字节十六进制参数值调整到相应的期望功率
- 所需频率和对应的十六进制数参数值请见频率参数值对照表 10-3
- 通过设置不同的当前工作频率，跳频最小值的最大值和通过跳频顺序数设置跳频模式(连续跳频模式或随机跳频模式)都可以启用跳频功能。禁止跳频，把所有的参数设置为 0 即可。
- 读/写

停止频率

- 设置读写器工作频率的上限
- 参数地址：0x0032
- 长度（Bytes）：4
- 初始值：0x374B9420（927.7MHz）
- 写入一 4 字节十六进制的参数值调整到所期望值。详见表 10-3 所示。
- 通过设置不同的当前工作频率，跳频最小值的最大值和通过跳频顺序数设置跳频模式(连续跳频模式或随机跳频模式)都可以启用跳频功能。禁止跳频，把所有的参数设置为 0 即可。
- 读/写

表 10-3 频率参照值对照表

频率(MHz)	十六进制参数值	描述
865.7	0x339988A0	EU 开始
866.7	0x33A8CAE0	EU 中
867.9	0x33BB1A60	EU 终止
902.3	0x35C80160	NA 开始
915.0	0x3689CAC0	NA 中
927.7	0x374B9420	NA 终止

跳频步长

- 当跳频启动时,用来调整跳频步长
- 参数地址：0x0034
- 长度（Bytes）：4
- 初始值：0x00030D40（200KHz）
- 通过设置不同的当前工作频率，跳频最小值的最大值和通过跳频顺序数设置跳频模式(连续跳频模式或随机跳频模式)都可以启用跳频功能。禁止跳频，把所有的参数设置为 0 即可。
- 读/写

跳频方式

- 通过先听后说的跳频方式参数在随机跳频和连续跳频之间切换
- 参数地址：0x0035
- 长度（Bytes）：1
- 初始值：0x01（随机跳频）
- 通过向该参数写入 0x01，选择随机跳频方式
- 通过向该参数写入 0x00，选择连续跳频方式
- 当处在连续跳频时,读定器采用先听后说(LSB)的方式
- 读/写

调制深度

- 用来设置读写器到标签的调制深度,通过公式(Vmax-Vmin)/Vmax 进行计算
- 参数地址：0x0036
- 长度（Bytes）：1
- 初始值：100%
- 调制深度值从 10%--100%以 10 为单位可调

- 调制深度参数值对照表如下 10-4 所示

表 10-4 调制深度参数表

调制深度%	十六进制参数
30	0x1E
80	0x50
90	0x5A
100	0x64

- 读写器的调制深度计算公式：

$(V_{MAX}-V_{MIN})/V_{MAX}$ V_{MAX}为最大发送功率下的RF电压; V_{MIN}为最小发送功率下的RF电压.(当调制深度为 100%时,V_{MIN}的值为零).

- 应用中具体标签所支持的调制深度,请参阅标签生产商给出的详细资料.
- 读/写

调制方式

- 使传输脉冲形状符合密集读写器模式或 ETSI 传输频谱
- 当要求频谱符合密集读写器模式/ETSI 302 208 时,给此参数写入 0x01
- 此模式只支持 IS0-18000-6B 标签;
- 若要运行在其它调制模式下,写入 0x00;
- 参数地址：0x0037
- 长度（Bytes）：1
- 初始值：0x00(无脉冲形状)
- 可读/可写

表 10-5 调整参考值

模式	十六进制参考值
无脉冲形状	0x00
ETSI	0x01
Japan(户内)	0x02
Japan(户外)	0x03

LBT 天线增益

控制接收器对话前监听的灵敏度

当监听其它传输信号时，设置此参数可以取消增益以外的一个外部天线

使用此参数只有与欧洲(ETSI)或日语区域设置,当 LBT 射频打开时

请勿使用此参数与 FCC 区域设置

参数地址：0x0038

长度（Bytes）：1
初始值：0x00(无 LBT 天线增益)
读/写
可用参数范围 0-255（0x00-0xFF）使用 8-bit 值
表现的范围为-127dbm - +127dbm .0x00-0x80 代表 0 - +128dbm 的范围,且值 0x81-0xFF 代表 -127- -1dbm 的范围（如表 10-6 所示）。

表 10-6 例 LBT 天线增益调整参数

十六进制参数值	天线增益(dBm)
0x81	-127
0x82	-126
…	…
0xFE	-2
0xFF	-1
0x00	0
0x01	+1
0x02	+2
…	…
0x7F	+127
0x80	+128

系统参数格式

读系统命令格式
表 10-7 读系统命令-ASCII 格式请求

系统参数	起始	标识符	命令	地址	块	校验	结尾
序列号	<CR>	0020	1201	0000	0004	calculated by user*	<CR>
固件版本	<CR>	0020	1201	0001	0004		
硬件版本	<CR>	0020	1201	0002	0004		
产品编码	<CR>	0020	1201	0003	0002		
读头 ID	<CR>	0020	1201	0004	0004		
读头名称	<CR>	0020	1201	0005	0020		
主机接口类型	<CR>	0020	1201	0006	0001		
主机接口波特率	<CR>	0020	1201	0007	0001		
用户端口路径	<CR>	0020	1201	0008	0001		
用户端口值	<CR>	0020	1201	0009	0001		
MUX 控制	<CR>	0020	1201	000A	0001		
运行模式	<CR>	0020	1201	000C	0001		
重试命令	<CR>	0020	1201	0011	0001		

功率	<CR>	0020	1201	0012	0001		
当前频率	<CR>	0020	1201	0030	0004		
起始频率	<CR>	0020	1201	0031	0004		
停止频率	<CR>	0020	1201	0032	0004		
跳频步长	<CR>	0020	1201	0034	0004		
跳频方式	<CR>	0020	1201	0035	0001		
调制深度	<CR>	0020	1201	0036	0001		
调制方式	<CR>	0020	1201	0037	0001		

*关于 CRC 的计算，参见 SkyeTek 协议 v3 参考指南

表 10-8 读系统命令-ASCII 模式请求

起始	响应码	数据长度	数据	CRC	结束
<LF>	1201	取决于系统参数	取决于系统参数	读写器自动计算	<CR><LF>

表 10-9 读系统命令 - 二进制格式请求

系统参数	STX	信息长度	标识符	命令	地址	快	CRC
序列号	2	calculated by user*	0020	1201	0000	0004	calculated by user*
固件版本	2		0020	1201	0001	0004	
硬件版本	2		0020	1201	0002	0004	
产品编码	2		0020	1201	0003	0002	
读头 ID	2		0020	1201	0004	0004	
读头名称	2		0020	1201	0005	0020	
主机接口类型	2		0020	1201	0006	0001	
主机接口波特率	2		0020	1201	0007	0001	
用户端口路径	2		0020	1201	0008	0001	
用户端口值	2		0020	1201	0009	0001	
MUX 控制	2		0020	1201	000A	0001	
运行模式	2		0020	1201	000C	0001	
重试命令	2		0020	1201	0011	0001	
功率	2		0020	1201	0012	0001	
当前频率	2		0020	1201	0030	0004	
起始频率	2		0020	1201	0031	0004	
停止频率	2		0020	1201	0032	0004	
跳频步长	2		0020	1201	0034	0004	
跳频方式	2		0020	1201	0035	0001	
调制深度	2		0020	1201	0036	0001	

调制方式	2		0020	1201	0037	0001	

*关于 CRC 的计算，参见 SkyeTek 协议 v3 参考指南

表 10-10 读系统命令 – 二进制格式请求

以下格式与所有读的格式一样

起始	信息长度	响应	数据长度	数据	CRC
<02>	0007	1201	取决于系统参数	取决于系统参数	读过读写器计算

写系统命令格式

表 10-11 写系统命令- ASCII 格式请求

系统命令	起始	标识符	命令	地址	块	数据长度	数据	CRC	结尾
序列号	<CR>	0820	1202	0000	0004	用户自定义	用户自定义	用户自己计算	<CR>
固件版本				0001	0004				
硬件版本				0002	0004				
产品编号				0003	0002				
读写器 ID				0004	0004				
读写器名称				0005	0020				
主机接口类型				0006	0001				
主机接口波特率				0007	0001				
用户端口路径				0008	0001				
用户端口值				0009	0001				
MUX 控制				000A	0001				
运行模式				000C	0001				
重试命令				0011	0001				
功率等级				0012	0001				
当前频率				0030	0004				
起始频率				0031	0004				
终止频率				0032	0004				
跳频步长				0034	0004				
跳频方式				0035	0001				
调制深度				0036	0001				
调制方式				0037	0001				

*关于 CRC 的计算，参见 SkyeTek 协议 v3 参考指南

表 10-13 写系统命令 – 二进制格式请求

系统参数	STX	信息长度	标识符	命令	地址	块	CRC

序列号	02	用户自定义计算	0820	1202	0000	0004	用户自定义计算
固件版本					0001	0004	
硬件版本					0002	0004	
产品编码					0003	0002	
读写器 ID					0004	0004	
读写器名称					0005	0020	
主机接口类型					0006	0001	
主机接口波特率					0007	0001	
用户端口路径					0008	0001	
用户端口值					0009	0001	
MUX 控制					000A	0001	
运行模式					000C	0001	
重试命令					0011	0001	
功率等级					0012	0001	
当前频率					0030	0004	
起始频率					0031	0004	
结束频率					0032	0004	
跳频步长					0034	0004	
跳频方式					0035	0001	
调制深度					0036	0001	
调制方式					0037	0001	

*关于 CRC 的计算，参见 SkyeTek 协议 v3 参考指南

STX:	信息长度	响应编码	CRC
<02>	0004	1202	<E652>

++++++++++++++++++++++++++++
/* 草稿版本，有待批阅及审核。 */
// 附录未翻，未完待续！
++++++++++++++++++++++++++++